File: priv_addr_thread

From: Luca Salgarelli [lsalgarelli@bell-labs.com]
Sent: Monday, January 17, 2000 10:11 AM
To: Sandra Thuel; Thomas Laporta; Ramachandran Ramjee; Kannan Varadhan
Subject: DHCP-MIP

Hi Folks.

So, I got the 10.* solution to the DHCP-MIP problem to work. In the process, I found a few points worth noting:

1) On a multi-homed HA, there must be an association between the client's NAI of the and the HA's interface on the client's home-network. This is needed because when the HA receives the encapsulated bcast packets, it needs to know on which interface the packets have to be forwarded. This (handling of incoming tunnelled bcast pkts.) should concern the MIP working group in general, so I'll send a note to Charlie & friends. Now the RFCs don't specify anything related, and a clarification on this point is needed independently from the use of DHCP.

2) There are another couple of details that I had to tweak on the HA to make it work. Normally, as a security feature, if a client has a home-addr that is not consistent with the network where the HA resides, forwarding of bcast packets is not allowed even if the client asks for it. This feature has to be turned off for 10.* addresses. In addition, normally the HA indexes the security-association list (the shared key for authentication) by home-address. In case of the NAI, it has to index using the NAI, of course, since the HA doesn't know the home-addr of the client in advance.

3) The ISI dhcp client uses a packet filter derived from the BPF to get DHCP packets. This doesn't work on a tunnelling interface, so I had to recompile the client with standard sockets.

These problems apart, the mechanism works OK.

Luca
From: Luca Salgarelli [lsalgarelli@bell-labs.com]
Sent: Monday, January 17, 2000 11:09 AM
To: Sandy Thuel
Cc: Thomas Laporta; Ramachandran Ramjee; Kannan Varadhan
Subject: Re: DHCP-MIP

Sandy:

> > 2) There are another couple of details that I had to tweak on the HA
> > to make it work. Normally, as a security feature, if a client has a
> > home-addr that is not consistent with the network where the HA
> > resides, forwarding of bca t allowed even if the
> > client asks for it. This f turned off for 10.*
> > addresses.

>
> This seems to be a problem many should have already encountered...
> Any idea as to whether the issue has been raised in any of the M-IP
> security drafts?

I don't think this is a rule written somewhere, I guess it's only common sense not to allow bcast packets coming from an interface that is not on the home-net of the client to be forwarded to the client. Since normally the HA has at least one of its interfaces on such network, I don't think this is an issue many people had the chance to experiment with. Probably we are the first ones to use a HA with a 10.* address :-)

> > In addition, normally the HA
> > indexes the security-association list (the shared key for
> > authentication) by home-address. In case of the NAI, it has to index
> > using the NAI, of course, since the HA doesn't know the home-addr of the client in advance.
>
> Again, this seems like something that should have come up in the
> context of the NAI work. Any idea if the NAI drafts comment on it?
> Perhaps we should post these issues on the M-IP mailing list? Or write
> to Charlie and Pat?

Although it is not clearly said, this is something that is already implied by the NAI draft. I don't think at this point it is worth asking for more precision on this issue.

> > 3) The ISI dhcp client uses a packet filter derived from the BPF to
> > get DHCP packets. This doesn't work on a tunnelling interface, so I
> > had to recompile the client with standard sockets.
>
> I thought you would use the Linux client rather than ISI's. Does it
> also use BPFs?

The Linux DHCP client's code explicitly states that it doesn't work on any interface different than an ethernet (not even a PPP or a Token Ring), so I didn't even look at that code.

> > These problems apart, the mechanism works OK.
>
> Any idea as to what the DHCP setup time is (i.e., the time from DHCP
> startup until a valid address is acquired and installed)?
> It would be interesting to compare the setup time for a power-up at
> home with that of a power up at a foreign domain. If you'd like, I
> can instrument and take some measurements soon. A qualitative
> comparison (e.g., number of messages/round trips) is nice but some
> timing results would be insightful and highlight the fact that we have
> implemented it.

Although I don't think taking those measurements should take long, I am out of the game: friday I received the confirmation from Xedia, and I'll be working with them to get the MIP (+ Hawaii, possibly) on their platform.

You're more than welcome to take the code, a Linux box, and continue on the measurements. Let me know and I can point you to the packages.

Luca

1